

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1 1. (Currently Amended) A digital wallet, secured with a user's access code,
2 for reproducing a confidential datum for said user, said digital wallet comprising:
3 (a) a computer-implemented input for receiving a input access code;
4 (b) a seed derivation module operatively connected to said input, for deriving
5 a seed usable to generate at least a portion of said confidential datum;
6 (c) a seed-based data generation module
7 (i) implementing a predetermined data generation protocol that was
8 previously used by a seed-based initialization of said confidential
9 datum of said user,
10 (ii) containing a representation of a seed-access code relationship,
11 (iii) configured to generate an output datum by digitally processing said
12 derived seed in accordance with said seed-access code relationship,
13 and
14 (iv) said output datum reproducing said at least a portion of said user's
15 confidential datum if said input access code equals said user's
16 access code; and
17 (d) said generation of said output datum occurring without dependence on any
18 storage of any form of said at least a portion of said confidential datum;
19 (e) wherein for at least one input access code not equaling said user's access
20 code, said output datum has the characteristic appearance of said at least a portion of said
21 confidential datum, but said output datum does not reproduce at least a portion of said user's
22 confidential datum.

1 2. (Canceled)

1 3. (Canceled)

1 4. (Original) The wallet of claim 1 where said access code is a PIN, and said
2 confidential datum includes an asymmetric cryptographic key.

1 5. (Original) The wallet of claim 4 where said output datum has the
2 characteristic appearance of an asymmetric cryptographic key.

1 6. (Original) The wallet of claim 1 where said access code is a PIN, and said
2 confidential datum includes a symmetric cryptographic key.

1 7. (Original) The wallet of claim 1 where said seed-access code relationship
2 is a identity relationship, so that said derived seed equals said input access code.

1 8. (Original) The wallet of claim 1 where said seed-access code relationship
2 represents said derived seed as a padded version of said input access code.

1 9. (Original) The wallet of claim 1 where said seed-access code relationship
2 includes a version of said initial seed masked by user's access code.

1 10. (Original) The wallet of claim 9 where:
2 (i) said masked version of said initial seed includes an XOR of said
3 initial seed with said user's access code; and
4 (ii) said processing of said derived seed in accordance with said seed-
5 access code relationship includes XORing said masked version of
6 said initial seed with said derived seed.

1 11. (Original) The wallet of claim 10 further comprising program code for
2 updating an user's old access code with a user's new access code by replacing said stored masked
3 version of said initial seed with its value XORed with said user's old access code XORed with
4 said user's new access code.

1 12. (Original) The wallet of claim 1 where:

2 (i) said seed-access code relationship includes a truncated version of
3 said initial seed capable of being concatenated with said input
4 access code to form said derived seed; and

5 (ii) said processing of said derived seed in accordance with said seed-
6 access code relationship includes concatenating said truncated
7 version of said initial seed with said input access code.

1 13. (Original) The wallet of claim 1 where:

2 (i) said seed-access code relationship includes values of, and
3 associations between, a plurality of possible values of said input
4 access code and a corresponding plurality of possible values of
5 said derived seed; and

6 (ii) said processing of said derived seed in accordance with said seed-
7 access code relationship includes looking up and outputting said
8 possible value of said derived seed corresponding to said input
9 access code.

1 14. (Original) The wallet of claim 13 where:

2 (1) said seed derivation module is merged with said data generation module;

3 (2) said output datum includes said derived seed.

1 15. (Original) The wallet of claim 5 where said confidential datum includes a
2 private key of said user, and said output datum has the characteristic appearance of a private key.

1 16. (Original) The wallet of claim 5 where said user's public key
2 corresponding to said user's private key is pseudo-public.

1 17. (Original) The wallet of claim 16 further comprising a digital certificate
2 containing said pseudo-public key.

1 18. (Original) The wallet of claim 17 where said digital certificate includes an
2 encrypted version of said user's pseudo-public key encrypted under a certifier's key which is not
3 verifiable except by authorized verifiers.

1 19. (Original) The wallet of claim 1 configured to be remotely accessible to a
2 roaming user across a network.

1 20. (Currently Amended) A computer-implemented method for securely
2 storing and reproducing a confidential datum for said user, comprising:

- 3 (a) receiving an input access code;
- 4 (b) deriving a seed usable to generate at least a portion of said confidential
5 datum by using said received input access code;
- 6 (c) obtaining a representation of a seed-access code relationship;
- 7 (d) digitally processing said derived seed
- 8 (i) in accordance with said seed-access code relationship,
- 9 (ii) by executing a predetermined data generation protocol that was
10 previously used by a seed-based initialization of said confidential
11 datum of said user,
- 12 (iii) thereby producing an output datum reproducing said at least a
13 portion of said user's confidential datum if said input access code
14 equals said user's access code; and
- 15 (e) said generation of said output datum occurring without dependence on any
16 storage of any form of said at least a portion of said confidential datum,
- 17 (f) wherein for at least one input access code not equaling said user's access
18 code, producing an output datum that has the characteristic appearance of said at least a portion
19 of said confidential datum, but said output datum does not reproduce at least a portion of said
20 user's confidential datum.

1 21. (Canceled)

1 22. (Canceled)

1 23. (Original) The method of claim 20 where said access code is a PIN, and
2 said confidential datum includes an asymmetric cryptographic key.

1 24. (Original) The method of claim 20 where said seed-access code
2 relationship is a identity relationship, so that said derived seed equals said input access code.

1 25. (Original) The method of claim 20 where said seed-access code
2 relationship represents said derived seed as a padded version of said input access code.

1 26. (Original) The method of claim 20 where said seed-access code
2 relationship includes a version of said initial seed masked by user's access code.

1 27. (Original) The method of claim 26 where:

2 (i) said masked version of said initial seed includes an XOR of said
3 initial seed with said user's access code; and

4 (ii) said processing of said derived seed in accordance with said seed-
5 access code relationship includes XORing said masked version of
6 said initial seed with said derived seed.

1 28. (Original) The method of claim 20 where:

2 (i) said seed-access code relationship includes a truncated version of
3 said initial seed capable of being concatenated with said input
4 access code to form said derived seed; and

5 (ii) said processing of said derived seed in accordance with said seed-
6 access code relationship includes concatenating said truncated
7 version of said initial seed with said input access code.

1 29. (Original) The method of claim 20 where:

- 2 (i) said seed-access code relationship includes values of, and
3 associations between, a plurality of possible values of said input
4 access code and a corresponding plurality of possible values of
5 said derived seed; and
6 (ii) said processing of said derived seed in accordance with said seed-
7 access code relationship includes looking up and outputting said
8 possible value of said derived seed corresponding to said input
9 access code.

1 30. (Original) The method of claim 29 where:

- 2 (1) said deriving said seed and said executing said predetermined data
3 generation protocol are merged into a common operation; and
4 (2) said output datum includes said derived seed.

1 31. (Canceled) A computer-readable medium having stored thereon a
2 program executable on a computer to securely store and reproduce a confidential datum for said
3 user, the program comprising computer logic instructions for:

- 4 (a) receiving an input access code;
5 (b) deriving a seed usable to generate at least a portion of said confidential
6 datum by using said received input access code;
7 (c) obtaining a representation of a seed-access code relationship;
8 (d) digitally processing said derived seed
9 (i) in accordance with said seed-access code relationship,
10 (ii) by executing a predetermined data generation protocol that was
11 previously used by a seed-based initialization of said at least a
12 portion of said confidential datum of said user,
13 (iii) thereby producing an output datum reproducing said at least a
14 portion of said user's confidential datum if said input access code
15 equals said user's access code; and

16 (e) said generation of said output datum occurring without dependence on any
17 storage of any form of said at least a portion of said confidential datum;

18 (f) wherein for at least one input access code not equaling said user's access
19 code, said output datum has the characteristic appearance of said at least a portion of said
20 confidential datum, but said output datum does not reproduce at least a portion of said user's
21 confidential datum.

1 32. (Canceled)

1 33. (Canceled)

1 34. (Original) The computer-readable medium of claim 31 where said access
2 code is a PIN, said confidential datum includes an asymmetric cryptographic key.

1 35. (Original) The computer-readable medium of claim 31 where said seed-
2 access code relationship is a identity relationship, so that said derived seed equals said input
3 access code.

1 36. (Original) The computer-readable medium of claim 31 where said seed-
2 access code relationship represents said derived seed as a padded version of said input access
3 code.

1 37. (Original) The computer-readable medium of claim 31 where said seed-
2 access code relationship includes a version of said initial seed masked by user's access code.

1 38. (Original) The computer-readable medium of claim 37 where:

2 (i) said masked version of said initial seed includes an XOR of said
3 initial seed with said user's access code; and

4 (ii) said processing of said derived seed in accordance with said seed-
5 access code relationship includes XORing said masked version of
6 said initial seed with said derived seed.

1 39. (Original) The computer-readable medium of claim 31 where:

- 2 (i) said seed-access code relationship includes a truncated version of
3 said initial seed capable of being concatenated with said input
4 access code to form said derived seed; and
5 (ii) said processing of said derived seed in accordance with said seed-
6 access code relationship includes concatenating said truncated
7 version of said initial seed with said input access code.

1 40. (Original) The computer-readable medium of claim 31 where:

- 2 (i) said seed-access code relationship includes values of, and
3 associations between, a plurality of possible values of said input
4 access code and a corresponding plurality of possible values of
5 said derived seed; and
6 (ii) said processing of said derived seed in accordance with said seed-
7 access code relationship includes looking up and outputting said
8 possible value of said derived seed corresponding to said input
9 access code.

1 41. (Original) The computer-readable medium of claim 40 where:

- 2 (1) said deriving said seed and said executing said predetermined data
3 generation protocol are merged into a common operation; and
4 (2) said output datum includes said derived seed.

1 42. (Currently Amended) A method for camouflaging a user's generation-
2 camouflaged access-controlled datum under said user's access code, comprising:

- 3 (a) initializing a user's access-controlled datum by using a generation protocol
4 in accordance with a generation indicia;
5 (b) storing in a memory in a digital wallet a predetermined relationship
6 between said generation indicia and said user's access code;

- 7 (c) camouflaging at least a portion of said access-controlled datum
8 (i) such as to be reproducible by an authorized user thereof but non-
9 reproducible by an unauthorized user thereof,
10 (ii) said camouflaging including storing said predetermined
11 relationship between said generation indicia and said user's access
12 code;
13 (iii) thereby allowing subsequent accessing of said at least a portion of
14 said access-controlled datum via computer-based processing of an
15 inputted access code, in accordance with said stored generation
16 indicia-access code relationship;
17 (iv) without dependence on any storage of any form of said at least a
18 portion of said access-controlled datum;
19 (v) wherein for at least one inputted access code not equaling said
20 user's access code, generating an output datum that has the
21 characteristic appearance of said at least a portion of said access-
22 controlled datum, but said output datum does not reproduce at least
23 a portion of said user's access-controlled datum; and
24 (d) ~~storing said camouflaged at least a portion of said access-controlled datum~~
25 ~~in a digital wallet; and~~
26 (e) —providing said digital wallet to said user.

- 1 43. (Original) A method for camouflaging a user's generation-camouflaged
2 access-controlled datum under said user's access code, comprising:
3 (a) initializing a user's access-controlled datum by using a generation protocol
4 in accordance with a generation indicia;
5 (b) generation-camouflaging at least a portion of said access-controlled datum
6 such as to be reproducible by an authorized user thereof but non-reproducible by an unauthorized
7 user thereof;

- 8 (c) storing said generation-camouflaged at least a portion of said access-
9 controlled datum in a digital wallet; and
10 (d) providing said digital wallet to said user.